

# United States District Court

## EASTERN DISTRICT OF OKLAHOMA

UNITED STATES OF AMERICA,

*Plaintiff,*

v.

NNAMDI FELIX UDEAGHA,

*Defendant.*

**CRIMINAL COMPLAINT**

Case No. 24-MJ-255-DES

I, Daniel Engelhardt, the undersigned complainant, state that the following is true to the best of my knowledge and belief.

In and around April 2021, and continuing through in and around December 2021, in the Eastern District of Oklahoma, NNAMDI FELIX UDEAGHA, committed the crime of Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code, Section 1349.

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

(See attached Affidavit of Daniel Engelhardt, which is attached hereto and made a part hereof by reference.)

☒ Continued on the attached sheet.



Daniel Engelhardt  
Special Agent  
Federal Bureau of Investigation



Sworn to on 8/1/2024

D. EDWARD SNOW

UNITED STATES MAGISTRATE JUDGE

Name and Title of Judicial Officer



Signature of Judicial Officer

**AFFIDAVIT IN SUPPORT OF  
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Daniel Engelhardt, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been employed by the FBI since October of 2023. I am currently assigned to the Oklahoma City Division, Cyber Squad. In this capacity, I am charged with investigating violations of federal criminal law to include computer intrusions and other crimes involving the use of computers.

2. Affiant is familiar with the facts and circumstances of this investigation. The statements made in this affidavit are based in part on: (a) my personal participation in this investigation; (b) information provided to me by other law enforcement officers; and (c) the training and experience of myself and other law enforcement agents and officers.

3. Since this affidavit is being submitted for the limited purpose of enabling a judicial determination of whether probable cause exists to justify the issuance of a criminal complaint, Affiant has not included each and every fact known to me and others concerning this investigation. Affiant has set forth only the facts that Affiant believes are essential to establish the necessary foundation for a criminal complaint.

4. Affiant submits that there is probable cause to believe that, from in and around April 2021, and continuing through in and around December 2021, in the Eastern District of Oklahoma and elsewhere, **NNAMDI FELIX UDEAGHA**, hereafter referred to as **UDEAGHA**, did knowingly and intentionally conspire and agree together with Uncharged Co-Conspirator-1 (hereafter UCC-1) and other persons known and unknown to the United States, to devise a scheme and artifice to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, to



transmit and cause to be transmitted by means of wire communications in interstate commerce certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

**FACTS SUPPORTING PROBABLE CAUSE**

5. The Chickasaw Nation is a federally recognized Indian Tribe, headquartered in Ada, Oklahoma, 74820, within the Eastern District of Oklahoma. The Chickasaw Nation operates numerous governmental entities for the benefit of its citizens, including the Chickasaw Nation Department of Health. The Chickasaw Nation Department of Health (hereafter “CNDH”) is headquartered in Ada, Oklahoma, within the Eastern District of Oklahoma.

6. Business-1<sup>1</sup> is a travel nursing staffing agency, with a headquarters located in Matairie, Louisiana. Business-1 utilizes a domain name of “www.giftedhealthcare.com” and emails from individuals working at Business-1 are sent from email addresses issued through that domain name. In and around 2021, the CNDH contracted with Business-1 to have Business-1 provide nursing staff to CNDH. Business-1 submitted periodic invoices to the Chickasaw Nation’s Department of Treasury, and the Department of Treasury would then pay Business-1 via electronic bank transfers from Vision Bank, located in Ada, Oklahoma, and within the Eastern District of Oklahoma.

Giftehealthcare.com

7. On or about December 8, 2021, the Chickasaw Nation Tribal Law Enforcement reported to the FBI that the Chickasaw Nation had been defrauded. According to the Chickasaw

---

<sup>1</sup> Through the Affidavit, Affiant has referred to this entity as Business-1 in an effort to protect the identity of the business.

Nation Tribal Law Enforcement, on or about December 7, 2021, the Chickasaw Nation's Information Technology security team received information that the Chickasaw Nation Department of Treasury had been defrauded through a suspected Business Email Compromise ("BEC") scam in which \$497,524.31 had been wired to unknown individual(s) utilizing a fraudulent domain name of "giftehealthcare.com."

8. On or about August 25, 2021, L.G., an employee with the CNDH, received an email from "Lcharouleau@giftehealthcare.com" asking to change the bank account to which CNDH sent electronic payments for Business-1. L.G. previously communicated with L.C., an actual employee at Business-1., via the email address Lcharouleau@giftedhealthcare.com regarding payments and billing. Legitimate emails from L.C. at Business-1. were sent from the domain "giftedheathcare.com." However, the email received on August 25, 2021, was sent from the domain name "giftehealthcare.com"—a domain name with the "d" missing from the word "Gifted."

9. L.G. replied to L.C. on August 25, 2021, and provided the unknown user(s) of "Lcharouleau@giftehealthcare.com" with the CNDH vendor direct deposit form. Shortly after, unknown user(s) of "Lcharouleau@giftehealthcare.com" replied to L.G. with a signed version of the form, along with what appeared to be a voided check from a Fifth Third Bank account ending in 0269.

10. On or about August 27, 2021, the Chickasaw Nation Department of Treasury transferred of \$32,298.50 from their account at Vision Bank, in Ada, Oklahoma, to the Fifth Third Bank account ending in 0269. The Chickasaw Nation Department of Treasury made this transfer believing that they were making payments owed to Business-1.

11. On or about September 16, 2021, the Chickasaw Nation Department of Treasury transferred \$126,687.75 from their account at Vision Bank, in Ada, Oklahoma, to the Fifth Third Bank account ending in 0269. The Chickasaw Nation Department of Treasury made this transfer believing that they were making payments owed to Business-1.

12. Records received from Fifth Third Bank show that the Fifth Third Bank account ending in 0269 is account held in the name "Wellshire Farms LLC." The sole signatory on the account is M.D.H., with an address in Michigan. The account was opened by M.D.H. on or about April 7, 2021. According to records from the Corporations Division of the Michigan Department of Licensing and Regulatory Affairs, Wellshire Farms, LLC was formed on or about April 5, 2021, with documents listing an address in Michigan and listing both M.D.H. and T.S. as agents in different portions of the documentation.

13. Further, records from Fifth Third Bank show that, after the Wellshire Farms LLC account ending in 0269 received the \$32,298.50 transfers from CNDH, the money was quickly moved out of the account over a period of five days.

14. Following the receipt of the \$126,687.75 transfer from CNDH on September 16, 2021, the money was again quickly moved out of the account over a short period of time.

15. On or about September 23, 2021, L.G. received another fraudulent email from "Lcharouleau@giftehealthcare.com." The email claimed that Business-1's bank account at Fifth Third Bank had been restricted and that Business-1 was changing financial institutions. The email included a new completed vendor account authorization form for JP Morgan Chase Bank and a payment information letter for a Chase account ending in 0335.

16. On or about September 29, 2021, a fourth fraudulent email was sent to L.G. from "Lcharouleau@giftehealthcare.com." The email contained a verification letter from Chase for



account ending in 0335. L.G. subsequently made arrangements to change Business-1's bank account information in the CNDH system for future payments. The CNDH subsequently sent the following payments intended for Business-1 from their bank account to the JP Morgan Chase bank account ending in 0335.

<u>Date</u>	<u>Amount</u>
September 30, 2021	\$816.00
October 14, 2021	\$242,079.30
October 21, 2021	\$65,003.88
November 10, 2021	\$30,638.88

17. Records from JP Morgan Chase Bank show that the JP Morgan Chase bank account ending in 0335 is an account held in the name "Geranium Modern LLC." The sole signatory on the account is M.H.<sup>2</sup>, with an address listed in Lilburn, Georgia. The account was opened by M.H. on or about August 3, 2021. According to record from the State of Georgia, Office of Secretary of State, Geranium Modern, LLC was created on April 21, 2021, with M.H. listed as both the registered agent and organizer.

18. Further, records from JP Morgan Chase show that, after the Geranium Modern LLC account ending in 0335 received the four transfers from CNDH listed above, the money was funneled out of the account in various ways.

#### **The Spoofed Website "Giftehealthcare.com"**

19. According to open source information, WHOIS.com is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database

---

<sup>2</sup> Affiant notes that, despite the similar initials, M.D.H. and M.H. are not the same individuals.

content in a human-readable format. According to WHOIS.com, “giftehealthcare.com” was registered on August 25, 2021, to an unnamed entity in Reykjavik, Iceland. WHOIS.com also indicated that NameCheap, Inc. (“NameCheap”) was the registrar for the domain.

20. On March 1, 2022, Magistrate Judge Kimberly E. West for the United States District Court for the Eastern District of Oklahoma, issued a search warrant to NameCheap for information related to the domain “giftehealthcare.com” (REDACTED). On or about March 16, 2022, NameCheap provided documents to the FBI pursuant to the search warrant.

21. The records received from NameCheap indicated that the individual who maintained the “giftehealthcare.com” domain was “John Rex,” using an email address of Email-1.<sup>3</sup>

22. Moreover, according to NameCheap’s website, Namecheap’s shared hosting, private email servers, VPS (Virtual Private Servers), and dedicated servers are located in Phoenix, Arizona. During the course of this investigation, Affiant spoke with L.G. L.G. confirmed that L.G. was physically located in the Eastern District of Oklahoma when L.G. received and sent emails to and from the fraudulent email address “Lcharouleau@giftehealthcare.com.” Therefore, Affiant submits that every email sent to or from the “Lcharouleau@giftehealthcare.com” to or from L.G., as described in further detail above, constitutes an interstate wire.<sup>4</sup>

23. On May 13, 2022, Magistrate Judge Kimberly E. West for the United States District Court for the Eastern District of Oklahoma, issued a search warrant to Google for

---

<sup>3</sup> For purposes of this publicly filed document, the underlying email address is referenced as “Email-1.”

<sup>4</sup> <https://www.namecheap.com/support/knowledgebase/article.aspx/136/22/where-are-your-datacenters-located-how-can-i-request-to-change-the-datacenter/>



information related to the email address Email-1 [REDACTED]. Records received from Google pursuant to the search warrant showed that this account was deleted on or about January 13, 2022, utilizing IP address 213.217.201.210.

24. NameCheap also provided a list of financial transactions which included payment information for the domain “giftehealthcare.com” and the other domains maintained by “John Rex.” NameCheap provided a record of a payment of \$50.00 that posted on November 10, 2021, from a credit card ending in 9957 listed in the name of UCC-1.<sup>5</sup> The records also showed that NameCheap received payment for John Rex’s domains from multiple cryptocurrency addresses. To allow this form of payment, NameCheap provides cryptocurrency addresses for users to send Bitcoin payments, and the users send Bitcoin from cryptocurrency addresses of their own to NameCheap’s cryptocurrency addresses. Based on the payments made to NameCheap’s cryptocurrency addresses, a Computer Scientist with the Federal Bureau of Investigation performed additional analysis and identified multiple addresses of interest.

25. The analysis revealed that the 23 cryptocurrency addresses provided by NameCheap were the Bitcoin addresses owned by NameCheap that received payments from “John Rex” for domain names, including “giftehealthcare.com.” The analysis revealed that two of NameCheap’s Bitcoin addresses, Bitcoin addresses ending in “dued” and “jrlm,” received payments from Binance for John Rex’s domain names. Binance is a cryptocurrency-exchange platform that allows users to convert currency to cryptocurrency and then transmit cryptocurrency to other addresses.

---

<sup>5</sup> Specifically, the records listed the first initial and the full last name of UCC-1.



26. Binance records identified the owner of the account that transferred money into the Bitcoin accounts ending in “dued” and “jrlm,” as UCC-1 (with a date of birth and passport number listed for UCC-1). Binance provided UCC-1’s telephone number and an email address—Email-2. Binance provided a list of approved devices that were utilized to operate the accounts on Binance. All of the approved devices listed by Binance were either iPhones or Mac Operating Systems. I know that both the iPhone and Mac Operating System are products offered by Apple. Binance records also indicated that a number of the approved devices utilized IP address 213.217.201.210 to operate on Binance. Access logs from the account provided by Binance indicated a large amount of activity utilizing the same IP address 213.217.201.210.

27. Records from Binance also confirmed that UCC-1’s Binance account was linked to the credit card ending in 9957 that was used to pay, in part, for the domains registered by “John Rex” and hosted by NameCheap. The Binance records included transaction records for this credit card, which showed a purchase on November 10, 2021, to “NAME CHEAP COM” in the amount of \$50.00. Binance records further showed several Fiat deposit transaction requests by UCC-1 utilizing a particular email address.<sup>6</sup> According to Businessinsider.com, Fiat money refers to government-issued currency that is not backed by a physical commodity, such as gold or silver, but rather by the government that issued it (such as U.S. dollar, the Euro, and other major global currencies). The Binance records show that Fiat money was deposited into UCC-1’s Binance account to fund the credit card ending in 9957 for the November 10, 2021, NameCheap transaction.

---

<sup>6</sup> Binance produced a partially redacted email address, which included the first three letters of the email address and then the domain/service provider (e.g., @gmail.com or @yahoo.com). All portions of the email address provided are consistent with Email-2.

28. In reviewing the cryptocurrency addresses provided by NameCheap, the FBI Computer Scientist also identified one of NameCheap's Bitcoin addresses—a Bitcoin address ending in "ryfe"—that received payment from an account at Blockchain.com. Blockchain.com is also a cryptocurrency-exchange platform that allows users to convert currency to cryptocurrency and then transmit cryptocurrency to other addresses. Records from Blockchain.com showed that the Blockchain.com account that made payments into NameCheap's Bitcoin account ending in "ryfe" was assigned to UCC-1, with a verified email address of Email-2. IP connection records provided by Blockchain.com indicated a login utilizing IP address 213.217.201.210 on November 29, 2021.

29. Records provided by Apple revealed that two iPhones were registered with Apple's iCloud service by UCC-1 using an Apple ID email address of Email-2. Records provided by Apple indicated that this user maintains an iCloud account and opted in for iCloud backup services. Records also indicated that UCC-1 conducted numerous transactions with the aforementioned iPhones utilizing email address Email-2 and IP address 213.217.201.210. This activity occurred between dates of August 2021 and July 2022.

30. On September 9, 2022, Magistrate Judge Kimberly E. West for the United States District Court for the Eastern District of Oklahoma, issued a search warrant to Apple for information related to the Apple iCloud account associated with "Email-2" [REDACTED]

31. A review of the records received from Apple related to the iCloud account for "Email-2" revealed numerous records related to the business email compromise scheme involving the Chickasaw Nation and Business-1. Specifically, those records included two PDF files, found within iCloud "Saved Documents," that were entitled "Check Remittance." The documents entitled "Check Remittance" appeared to be documents on Chickasaw Nation Department of



Health letterhead detailing transactions for travel nursing. The documents set out a description of the services provided to CNDH by Business-1, as well as the dates and costs associated with each service. The documents further document that CNDH was issuing payment to Business-1 for those specific services. One of documents entitled "Check Remittance" detailed seven transactions, with a total cost to CNDH of \$65,003.88, for which CNDH issued payment to Legal-Name-Business-1, dba Business-1, on October 21, 2021. The second document entitled "Check Remittance" detailed twenty-seven transactions, for a total cost to CNDH of \$126,687.75, for which CNDH issued payment to Legal-Name-Business-1, dba Business-1, on September 16, 2021.

32. In addition to the actual PDF documents, the iCloud returns also contained a screenshot taken on a phone of another "Check Remittance" document from C.N. Division of Health. This image detailed one transaction, for a total cost to CNDH of \$816.00. CNDH issued payment to Legal-Name-Business-1, dba Business-1, on September 30, 2021. Another image on the phone appeared to be a picture taken of a computer screen which displayed part of a "Check Remittance" document. The image captured showed a listed check number of REMIT00000000012762, which listed five transactions and in the total amount of \$32,298.50.

33. A review of images found in the iCloud data showed three images taken of a computer screen showing the email threads between L.C. and the individual masquerading as "L.G." who was using the fraudulent email address "Lcharouleau@giftehealthcare.com." One of these images contained a date and time stamp indicating that it was created on September 23, 2021, at 8:43 a.m. A second image contained a date and time stamp indicating that it was created on September 27, 2021, at 3:14 p.m. Affiant notes that both dates and times are within the time period of when the fraud scheme was occurring.

34. A review of stored WhatsApp messages contained in the iCloud data for the Apple account for "Email-2" showed that the user of that account—UCC-1—exchanged messages with an individual with the WhatsApp username, GxQ, which is assigned to WhatsApp phone number +[REDACTED]1871.

35. Based on the following information the Affiant submits there is probable cause to believe GxQ is Nnamdi Felix **Udeagha**. Records from Apple show **Udeagha's** iCloud account was created on September 11, 2018 for the phone number +[REDACTED]1871; however, records to date provided by Apple do not show what date(s) the phone number was verified.

36. On August 9, 2021, at approximately 4:39 p.m., GxQ sent the following message to UCC-1:

"Business name: Wellshire Farms LLC  
Bank Name: Fifth Third Bank  
Account number: [REDACTED]0269  
ACH Routing: 072405455  
Wire Routing: 042000314  
Bank Address: 4501 [REDACTED], Detroit, MI 48201  
Beneficiary Address: [REDACTED] Detroit, MI 48219"

UCC-1 immediately responded with two messages, both sent at approximately 4:39 p.m.:

"Okay"

"I'm on it"

Based on your Affiant's training and experience, Affiant understands that the user of GxQ provided UCC-1 with information for a bank account into which UCC-1 could direct the victim, CNDH, to send payments. Affiant further understands that UCC-1 confirmed that he would use the account provided by GxQ.



37. As set forth in greater detail above, on August 25, 2021, the user of the fraudulent email address "Lcharouleau@giftehealthcare.com" directed CNDH to send payments to this exact Fifth Third Bank account listed in the message from GxQ to UCC-1.

38. On September 16, 2021, at approximately 1:08 p.m., UCC-1 sent GxQ the following messages:

"A document titled, C.N. Division of Health\_REMIT000000000128777"

"Nwanne<sup>7</sup> 126k"

"Wellshire"

"Let's gooooo!"

"Business Name: Wellshire Farms LLC

Bank Name: Fifth Third Bank

Account number: [REDACTED] 0269

ACH Routing: 072405455

Wire Routing: 042000314

Bank Address: 4501 [REDACTED] Detroit, MI 48201

Beneficiary Address: 19306 [REDACTED] Detroit, MI 48219"

"Confirm me tomorrow biko<sup>8</sup>"

Based on Affiant's training, experience and knowledge of this investigation, Affiant believes that UCC-1 sent this series of messages to GxQ to let GxQ know that CNDH had sent UCC-1 a document showing that CNDH had made a payment of \$126,000.00 into the Fifth Third Bank Account. Affiant notes that UCC-1 attached one of the "Check Remittance" documents

---

<sup>7</sup> Based on Affiant's training and experience, and a review of the website [https://nkowaokwu.com/word?word=nwanne#:~:text=1.,\(s\)%20%2D%20brother%2C%20sister](https://nkowaokwu.com/word?word=nwanne#:~:text=1.,(s)%20%2D%20brother%2C%20sister), Affiant understands "Nwanne" to be a Nigerian Igbo word meaning, sibling, which is used in slang to describe a close friend.

<sup>8</sup> Based on Affiant's training and experience, and a review of the website <http://naijalingo.com/words/biko>, Affiant understands "biko" to be a Nigerian Igbo word meaning please.

described above to this message. Affiant believes that UCC-1 requested that GxQ confirm the money was, in fact, received into the Fifth Third bank account.

39. On September 23, 2021, at approximately 11:55 a.m., UCC-1 sent GxQ the following messages:

“But that wellshire”

“Wey cast that 100k job<sup>9</sup>”

“I wan (sic) update the account”

“Them suppose pay today”

Based on Affiant’s training, experience and knowledge of this investigation, Affiant believes that in the above-listed messages, UCC-1 reached out to user GxQ to let GxQ know that there was a problem with the Fifth Third Bank Account ending in 0269, which was opened in the name of Wellshire Farms LLC. Affiant believes that UCC-1 then requested that GxQ create a new account, because CNDH was supposed to make a payment that same day.

40. As set forth in greater detail above, the account holder of the Fifth Third Bank Account ending in 0269, withdrew a substantial sum of cash within days of receiving the second transfer from CNDH.

41. Later, on that same day, at approximately 11:57 a.m., GxQ responded with the following messages:

“Shit”

---

<sup>9</sup> Based on Affiant’s training and experience, and a review of the website [naijalingo.com/words/cast](http://naijalingo.com/words/cast), Affiant understands that the word “cast” means to spoil or fail in Nigerian Pidgin.



“Make I get Aza<sup>10</sup>?”

UCC-1 responded almost immediately, also at 11:57 a.m., with the following message:

“Yes”

Based on Affiant’s training, experience and knowledge of this investigation, Affiant believes that in the above-listed messages, GxQ asked UCC-1 to confirm that GxQ should set up a new bank account into which UCC-1 could direct CNDH to deposit further payments to Business-1. Affiant further believes that UCC-1 replied to confirm that UCC-1 wanted GxQ to set up a new bank account for the fraud scheme.

42. On the same day, September 23, 2021, at approximately 12:27 p.m., GxQ sent UCC-1 the following message:

“Chase

Geranium Modern LLC

Bank Address: 4170 [REDACTED] Alpharetta, GA, 30005

Beneficiary Address: 876 [REDACTED] Lilburn, GA, 30047

Account number: [REDACTED] 0335

Routing number: 072000326”

Based on Affiant’s training, experience and knowledge of this investigation, Affiant believes that in the above-listed message, GxQ provided UCC-1 with information for a new bank account that was prepared to receive the proceeds of the fraud scheme.

---

<sup>10</sup> Based on Affiant’s training and experience, and a review of the website [en.wikipedia.org/wiki/Aza\\_\(slang\)](https://en.wikipedia.org/wiki/Aza_(slang)), Affiant knows that “Aza” is a Nigerian slang term used to describe a bank account or bank account number.

43. As set forth in greater detail above, the Chase bank account provided by GxQ is the same bank account to which CNDH was directed to transmit future payments with respect to Business-1.

44. On October 21, 2021, at approximately 1:02 p.m., GxQ sent UCC-1 the following message:

“242,000 hang inside. He just called me to tell me”

GxQ immediately sent a second message that contained an image. Due to limitations with law enforcement’s technical ability to parse these messages out of iCloud return data, Affiant cannot determine with absolute certainty which image within the Email-2 iCloud account was received via this message from GxQ. However, Affiant located an image within the return that is marked with a date stamp of October 21, 2021, that shows a person holding a phone showing the Chase Bank application open. The image shows that the Chase Bank application is logged into an account ending in 0335 and shows that the most recent transaction was in the amount of \$240,271.74 associated with the following entry:

“ORIG CO NAME: CN HEALTH SYSTEM CO ENTRY DESCR: PAYABLES SEC: PPD”

Based on Affiant’s training, experience and knowledge of this investigation, Affiant submits that this image is a picture of an unknown individual who directly accessed the JP Morgan Chase bank account ending in 0335 into which CNDH made payments from the wire fraud.

45. Based on my training, experience and knowledge of the case, these messages show UCC-1 reaching out to GxQ for the financial institution information used to facilitate the fraudulent transactions and GxQ responding with the accounts to use. Therefore, I believe GxQ is facilitating the financial side of the fraud by providing bank accounts attached to shell companies.



### IDENTIFICATION OF UDEAGHA AS “GxQ”

46. A review of law enforcement databases show that a Texas State Identification card (Texas ID Number [REDACTED]) is issued to Nnamdi Felix **Udeagha**, at a listed address of 18303 [REDACTED] Humble, Texas 77346.<sup>11</sup>

47. On or about April 30, 2024, Nnamdi Felix **Udeagha** purchased a BMW 5-Series Sedan from BMW of Houston North. On his auto purchase application, **Udeagha** listed his address as “18303 [REDACTED] Houston, Texas.” Affiant notes that Humble, Texas, is considered to be a suburb of Houston, Texas. Moreover, **Udeagha** listed his phone number on the auto loan application as [REDACTED]-3764.

48. Records provided by Apple indicate that a user with a verified phone number of, +[REDACTED]1871—the WhatsApp number<sup>12</sup> in communication with UCC-1—maintains an iCloud account with Apple. This iCloud account is assigned an iCloud email address of udeaghannamdi@icloud.com and has listed address of 18303 [REDACTED], Humble, Texas 77346. This account also lists a second phone number of +[REDACTED]3764. Furthermore, the records from Apple show that the user of this iCloud account has multiple billing payments made using a Mastercard, a Visa credit card, and a Paypal account. The records show that the accounts are all held in the name “Nnamdi Udeagha” and all three accounts list an address of

---

<sup>11</sup> Through surveillance and other sources of information, law enforcement believes that **Udeagha** in fact resides at a different property in the Houston, Texas area. However, property records show that the residence located at 18303 [REDACTED] Humble, Texas 77346 is owned by the individual **Udeagha** listed on his BMW auto loan application as his sister.

<sup>12</sup> Records from WhatsApp indicated that Udeagha’s account wasn’t created until 2022, however based on my training and experience, I know that WhatsApp accounts can be frequently created and deleted when loading the application on new devices at the users request.

18303 [REDACTED] Humble, Texas 77346. Apple records indicated that the iCloud account was created in 2018 and maintained a verified phone number of +[REDACTED]1871, although records do not indicate when the phone number was verified.

49. In addition, in or around the time of November 25, 2021 at approximately 1:15:04 PM the message from GxQ sent the following message to UCC-1 which identified GxQ as Nnamdi Felix **Udeagha**:

“The man don (sic) look my account”

“Zenith

Nnamdi **Udeagha**

[REDACTED]1358”

Based on my training, experience, and knowledge of the case, I know that Zenith is a common bank headquartered in Nigeria and the context of the message indicates GxQ is sending personal bank account details in anticipation of a transaction. These messages not only identifies GxQ to be Nnamdi Felix **Udeagha**, but also directs UCC-1 to send funds to his personal account, which is in the name of “Nnamdi **Udeagha**”.

### **CONCLUSION**


50. Based on the above information and the totality of the circumstances, Affiant submits there is probable cause to establish that, from in and around April 2021, and continuing through in and around December 2021, in the Eastern District of Oklahoma and elsewhere, **NNAMDI FELIX UDEAGHA**, did knowingly and intentionally conspire and agree together and with UCC-1 and other persons known and unknown to the United States, to devise a scheme and artifice to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, to



transmit and cause to be transmitted by means of wire communications in interstate commerce certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

  
\_\_\_\_\_  
Daniel Engelhardt  
FBI, Special Agent

Subscribed and sworn to before me on August 1, 2024

  
\_\_\_\_\_  
UNITED STATES MAGISTRATE JUDGE